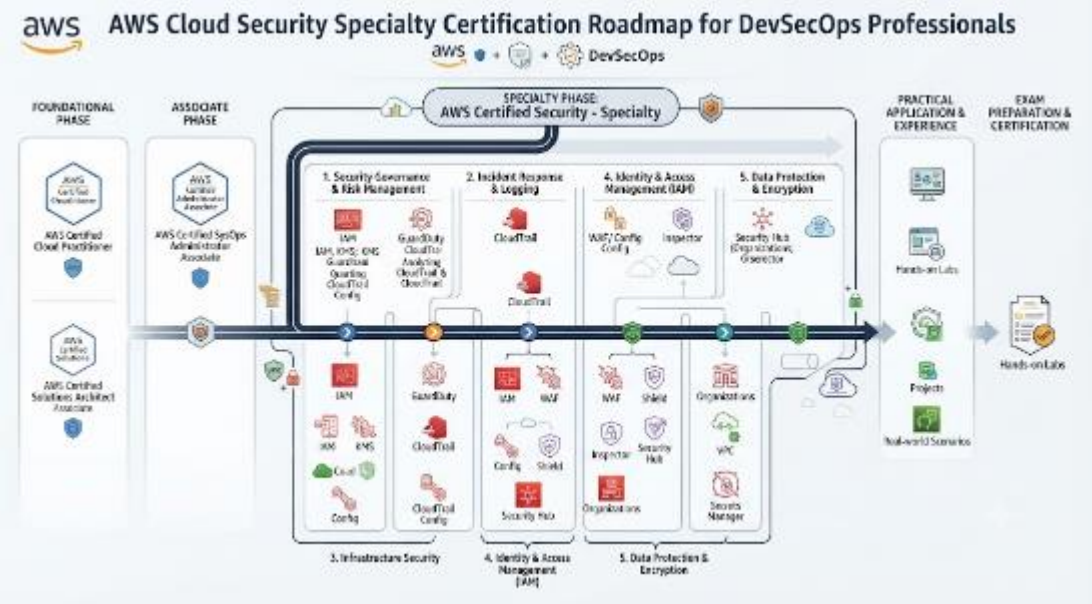
AWS Cloud Security Specialty Certification Roadmap for DevSecOps Professionals



Introduction

Security has become a core responsibility for every professional working with cloud platforms. Developers must protect application credentials, DevOps engineers must secure deployment pipelines, architects must design protected infrastructure, and managers must ensure that cloud systems follow business and compliance requirements.AWS Certified Security – Specialty is designed for professionals who want deeper knowledge of security within Amazon Web Services. It covers identity protection, encryption, threat detection, incident handling, network security, monitoring and cloud governance.The earlier SCS-C02 exam has now moved to the SCS-C03 version. However, the main security concepts remain useful for professionals preparing for AWS cloud security roles.

Certification at a Glance

Information	Details
Certification name	AWS Certified Security – Specialty
Track	Cloud Security and DevSecOps
Level	Advanced
Suitable for	Engineers, developers, architects, security professionals and managers
Basic requirements	AWS knowledge, networking, IAM, encryption and security fundamentals

Information	Details
Main skills	Access control, data protection, monitoring, incident response and governance
Suggested learning order	AWS fundamentals → Cloud operations → Security concepts → Specialty preparation
Provider	DevOpsSchool

What Is AWS Certified Security Specialty?

AWS Certified Security – Specialty is an advanced certification focused on protecting cloud workloads.

It checks whether a candidate can secure AWS accounts, users, applications, networks and data. It also measures the ability to respond to security threats and maintain governance across cloud environments.

This certification is useful for professionals who already understand AWS services and want to specialise in cloud security.

Who Should Consider This Certification?

This certification is suitable for people working in technical and management roles, including:

- Cloud security engineers
- DevOps engineers
- DevSecOps professionals
- Software developers
- Cloud architects
- Platform engineers
- Site reliability engineers
- System administrators
- Security analysts
- Technical managers
- Governance and compliance professionals

It is especially useful for professionals responsible for protecting production workloads, customer information, cloud accounts and deployment systems.

Recommended Prerequisites

There is no compulsory certification required before starting this path. However, candidates should understand basic AWS services and security concepts.

Useful knowledge includes:

- Amazon EC2, S3, RDS and Lambda
- Amazon VPC and network routing
- AWS Identity and Access Management
- CloudTrail and CloudWatch
- Encryption and key management
- Security groups and network ACLs
- Authentication and authorisation
- Shared responsibility in cloud computing

Practical AWS experience makes the certification easier to understand because many questions are based on real situations.

Important Skills Covered

Identity and Access Security

Candidates learn how to control access to AWS resources. This includes IAM users, roles, policies, permission boundaries, temporary credentials, federation and cross-account access.

The main objective is to give users and services only the permissions they genuinely need.

Data Protection and Encryption

This section focuses on securing sensitive information.

Candidates study encryption at rest, encryption in transit, AWS KMS, secrets management, certificates, key rotation and protected storage.

Infrastructure and Network Protection

Secure cloud systems need protected networks and controlled communication.

Professionals learn about VPC design, private subnets, security groups, network ACLs, VPC endpoints, AWS WAF, AWS Shield and firewall services.

Monitoring and Threat Detection

Cloud security requires continuous visibility.

Candidates learn how services such as CloudTrail, GuardDuty, Security Hub, AWS Config and CloudWatch help detect suspicious activities, policy violations and unusual behaviour.

Incident Response

This area explains how to react when a security problem occurs.

Professionals must know how to isolate resources, preserve evidence, investigate logs, remove threats and safely restore services.

Governance and Compliance

Large organisations often operate many AWS accounts.

Candidates learn how to apply security rules across multiple accounts, monitor compliance, collect audit evidence and use organisational controls.

Skills You Will Gain

After completing the learning process, you should be able to:

- Create secure AWS account structures
- Build least-privilege access policies
- Configure secure cross-account access
- Protect privileged identities
- Encrypt files, databases and backups
- Manage encryption keys and application secrets
- Detect suspicious cloud activities
- Investigate security alerts
- Secure networks and application traffic
- Protect web applications from common attacks
- Centralise security findings
- Automate security actions
- Apply governance policies
- Support compliance and audit activities
- Secure development and deployment pipelines

Practical Projects to Build

Hands-on projects improve both examination preparation and job readiness.

Useful projects include:

- Creating an IAM model for different teams
- Building a secure multi-account environment
- Setting up centralised CloudTrail logging
- Configuring GuardDuty and Security Hub
- Encrypting S3 buckets and databases
- Creating automatic secret rotation
- Designing a VPC with private workloads
- Protecting an application with AWS WAF
- Building security alerts with CloudWatch

- Creating an incident response workflow
- Automating remediation for risky configurations
- Preparing a cloud security assessment report

These projects help candidates explain their knowledge during interviews and workplace discussions.

Preparation Options

7–14-Day Preparation

This approach is suitable for experienced AWS professionals.

Focus on:

- IAM and access control
- Encryption and AWS KMS
- CloudTrail and GuardDuty
- Security Hub and incident response
- VPC security
- Governance and compliance
- Practice questions and revision

Candidates using this plan should already have practical AWS security experience.

30-Day Preparation

This plan works well for working engineers.

Week 1: IAM, roles, policies and account security
Week 2: Encryption, secrets and network protection
Week 3: Monitoring, detection and incident management
Week 4: Governance, hands-on labs and practice tests

A daily study schedule of around one hour is usually manageable for working professionals.

60-Day Preparation

This option is better for learners who need more practice.

Days 1–10: AWS and networking fundamentals
Days 11–20: IAM and authentication
Days 21–30: Encryption and data protection
Days 31–40: Infrastructure and application security

Days 41–50: Monitoring and incident response
Days 51–60: Governance, projects and exam practice

Common Preparation Mistakes

Candidates should avoid the following errors:

- Studying only through memorisation
- Ignoring practical AWS labs
- Giving broad permissions instead of least privilege
- Depending on permanent access keys
- Confusing monitoring tools with investigation tools
- Ignoring key policies in AWS KMS
- Removing compromised resources before preserving evidence
- Studying only IAM and encryption
- Avoiding governance and compliance topics
- Using outdated exam material without checking changes
- Selecting complicated solutions when a simpler secure option exists
- Taking practice tests without reviewing incorrect answers

Choose Your Learning Path

DevOps

Begin with AWS fundamentals, Linux, CI/CD and infrastructure as code. Then learn cloud security, secure automation and professional DevOps practices.

DevSecOps

Focus on application security, secure pipelines, vulnerability scanning, secrets management, policy as code and automated security controls.

SRE

Combine reliability engineering with access security, monitoring, incident response, production protection and service recovery.

AIOps and MLOps

Learn secure machine-learning pipelines, protected data access, model permissions, monitoring and automation.

DataOps

Focus on secure databases, encryption, access control, data governance, audit logging and protected data movement.

FinOps

Combine account governance, cost control, tagging, resource policies and risk management to protect both systems and cloud budgets.

Best Certification to Pursue Next

The next certification should match your job role.

DevOps professionals can move toward an advanced AWS DevOps certification. Cloud architects can continue with a professional architecture path. Network specialists may choose advanced cloud networking, while security professionals can expand into DevSecOps, governance or incident response.

The right next step depends on whether your main goal is architecture, operations, development, security or management.

Training and Certification Support Institutions

DevOpsSchool

DevOpsSchool provides structured learning for AWS, DevOps, DevSecOps, cloud security and automation. Its training approach is suitable for working professionals who need guided sessions, practical labs and certification support.

Cotocus

Cotocus supports cloud engineering, digital transformation and enterprise technology learning. It may help organisations and professionals connect cloud security knowledge with broader business and engineering requirements.

Scmgalaxy

Scmgalaxy offers resources related to DevOps tools, configuration management, automation and cloud technologies. These areas help learners build the technical foundation required for AWS security.

BestDevOps

BestDevOps focuses on DevOps practices, engineering knowledge, learning roadmaps and professional skills. It can support learners interested in combining AWS security with automation and platform engineering.

DevSecOpsSchool

DevSecOpsSchool is relevant for professionals who want to include security in software development and deployment. Its learning areas include secure pipelines, application protection and cloud security automation.

SRESchool

SRESchool supports learning in observability, reliability, incident management and production operations. These skills are useful for AWS security monitoring and response roles.

AIOpsSchool

AIOpsSchool focuses on automation and artificial intelligence in IT operations. It helps learners understand monitoring, event analysis and intelligent operational processes.

DataOpsSchool

DataOpsSchool covers data engineering, workflow automation, governance and data operations. It is useful for professionals responsible for securing cloud-based data systems.

FinOpsSchool

FinOpsSchool focuses on cloud financial management, governance and cost optimisation. It helps professionals understand how security decisions can also affect financial control.

Conclusion

AWS Certified Security – Specialty is a strong learning path for professionals who want to protect modern cloud environments. It develops practical skills in identity management, encryption, monitoring, network security, incident response and governance. The certification is suitable for engineers, developers, architects, managers and security professionals. Effective preparation should include clear concepts, hands-on projects and scenario-based practice. Learners should also ensure that their preparation reflects the latest SCS-C03 exam while using older SCS-C02 material only for relevant foundational topics.